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

基于GaAs/$Al_{0.45}Ga_{0.55}As$超晶格芯片自发混沌振荡的8Gb/s物理真随机数实现

刘延飞 陈诚 杨东东 李修建

Generation of 8Gb/s physical random numbers based on spontaneous chaotic oscillation of GaAs/$Al_{0.45}Ga_{0.55}As$ superlattices

Liu Yan-Fei Chen Cheng Yang Dong-Dong Li Xiu-Jian

引用信息 Citation: Acta Physica Sinica, 69, 100504 (2020) DOI: 10.7498/aps.69.20200136
在线阅读 View online: https://doi.org/10.7498/aps.69.20200136
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于 $GaAs/Al_{0.45}Ga_{0.55}As$ 超晶格芯片自发混沌振荡的 8 Gb/s 物理真随机数实现*

刘延飞[1)] 陈诚[1)] 杨东东[1)†] 李修建[2)]

1) (火箭军工程大学基础部, 西安 710025)

2) (国防科技大学文理学院, 长沙 410073)

(2020 年 1 月 19 日收到; 2020 年 3 月 14 日收到修改稿)

物理真随机数发生器对密码学和保密通信至关重要. 现有随机数发生器, 或者复杂庞大, 或者受限于器件带宽, 不能很好地满足现代高速通信系统的需要. 本文提出了一种基于超晶格 (superlattices, SLs) 芯片的全固态实时高速物理真随机数发生器. 通过选取合适直流偏置电压对 SLs 芯片进行激发, 从而产生高频混沌振荡信号作为物理熵源, 利用采样频率为 2 GHz 的多位模数转换器 (analog-to-digital converter, ADC) 进行量化, 生成 12 位的二进制随机比特, 然后使用现场可编程逻辑门阵列 (field programmable gate array, FPGA) 抽取最低 4 位为有效位并进行比特反转以改善其随机性, 最终获得了实时速率为 8 Gbit/s 的随机数. 经验证, 该发生器产生的随机数通过了随机数行业标准 (NIST SP 800-22) 的测试, 具备优良的统计特性, 有望小型化集成到高速通信设备之上.

关键词: 超晶格, 自发混沌振荡, 物理真随机数, 多位采样

PACS: 05.40.–a, 73.21.Cd, 05.45.–a, 68.65.Cd **DOI:** 10.7498/aps.69.20200136

1 引 言

随机数在蒙特卡洛模拟、密码学、数字认证、保密通信等领域发挥着至关重要的作用[1,2]. 在保密通信中, 在使用对称密码、公钥密码、消息认证码、数字签名等密码技术时, 都需要使用密钥, 一般利用随机数作为密钥对原始信息进行加密. 根据香农的理论[3], 只要密钥完全随机, 与所要加密的信息长度一致且一次使用, 理论上完全不可破解, 因此快速产生安全可靠的随机数是保密通信系统的关键. 按照产生方式不同, 随机数可分为真随机数和伪随机数[4]. 伪随机数通过确定性算法产生[5], 具有周期性与可复现性. 物理真随机数发生器基于物理随机现象, 能够产生无法预知、不可再现的真随机数[6].

传统物理真随机数发生器主要基于电路热噪声[7,8]、压控振荡器[9]、混沌电路[10,11]等物理熵源, 但受限于这些物理信号的带宽, 产生的随机数速率多处于 Mbit/s 级别, 很难满足现代通信系统对高速随机数的要求. 近年来利用混沌激光作为物理熵源, 得到了离线速率高达 100 Gbit/s[12], 300 Gbit/s[13] 和实时速率达到 14 GBit/s[14], 20 GBit/s[15] 的随机数. 但混沌激光系统复杂, 成本高, 且需要外部反馈, 涉及电-光和光-电双重转换, 容易受到外界因素的干扰, 因此混沌激光随机数发生器无法小型化集成到保密通信设备之上.

超晶格 (superlattices, SLs) 是用两种晶格匹配度很好的半导体材料周期性交替生长而成的全固态电子器件, 最早由 IBM 公司的 Esaki 和

* 国家自然科学基金重点项目 (批准号: 61834004) 资助的课题.

† 通信作者. E-mail: yd_xian@163.com

Chang[16] 提出. 中科院张耀辉团队 [17–19] 在国际上率先发现 GaAs/$Al_{0.45}Ga_{0.55}As$ SLs 在液氮温区及室温条件下直流偏置电压的自发混沌振荡现象. 国内外诸多学者通过对 GaAs/$Al_{0.45}Ga_{0.55}As$ SLs 的结构 [20] 以及自发混沌振荡现象 [21,22] 的研究, 证实了 SLs 是理想的混沌噪声源, 可以产生真随机数, 其随机数产生速率可达 80 Gbit/s[23].

本文提出了一种基于 SLs 芯片的实时高速物理真随机数发生器. 首先, 以 SLs 物理熵源为核心, 搭建了 SLs 高速物理真随机数产生装置. 通过对信号的混沌特性进行分析选择合适的直流偏置电压, 随后使用采样速率为 2 GHz 的 12 位高速模数转换器 (analog-to-digital converter, ADC) 对 SLs 信号进行采集量化得到随机比特. 接着使用现场可编程逻辑门阵列 (field programmable gate array, FPGA) 从 12 位随机比特中抽取最低 4 位作为有效位进行比特反转. 最终获得了实时速率为 8 Gbit/s 的随机数, 并且该随机数具有良好的统计随机特性, 可满足现代通信系统对高速率随机数的需求.

2 SLs 高速物理真随机数产生方案

2.1 SLs 结构

为方便实验调试, 本文使用的 SLs 封装成双列直插式, 如图 1(a) 所示, 其尺寸大小约为 1.5 mm × 1.5 mm(圆圈内). 图 1(b) 为 SLs 的结构示意图, SLs 由 50 周期的弱耦合势阱 (GaAs) 和势垒 ($Al_{0.45}Ga_{0.55}As$) 组成 [23], 夹于两个 300 nm 硅基 GaAs 层中形成了 n^+-n-n^+的二极管结构 [19]. $Al_{0.45}Ga_{0.55}As$ 势垒层厚度为 4 nm, GaAs 势阱层总厚度为 7 nm, 其中掺杂硅基 GaAs 层两侧各有 2 nm 厚的无掺杂 GaAs 层, 以防止硅原子扩散到相邻 $Al_{0.45}Ga_{0.55}As$ 势垒层. 虽然这些结构是周期性的, 但是在生长过程中, 其层厚、掺杂浓度等不可避免地存在随机涨落, 因此构成了一个极大自由度的随机非线性系统. 交替生长的 GaAs 和 $Al_{0.45}Ga_{0.55}As$ 材料具有不同的禁带宽度, 它们分别构成了量子阱的阱和垒, 其能带结构示意图如图 1(c) 所示. 在弱耦合 SLs 中, 电荷被局限在各个量子阱中, 电荷的输运通过各个相邻量子阱间的共

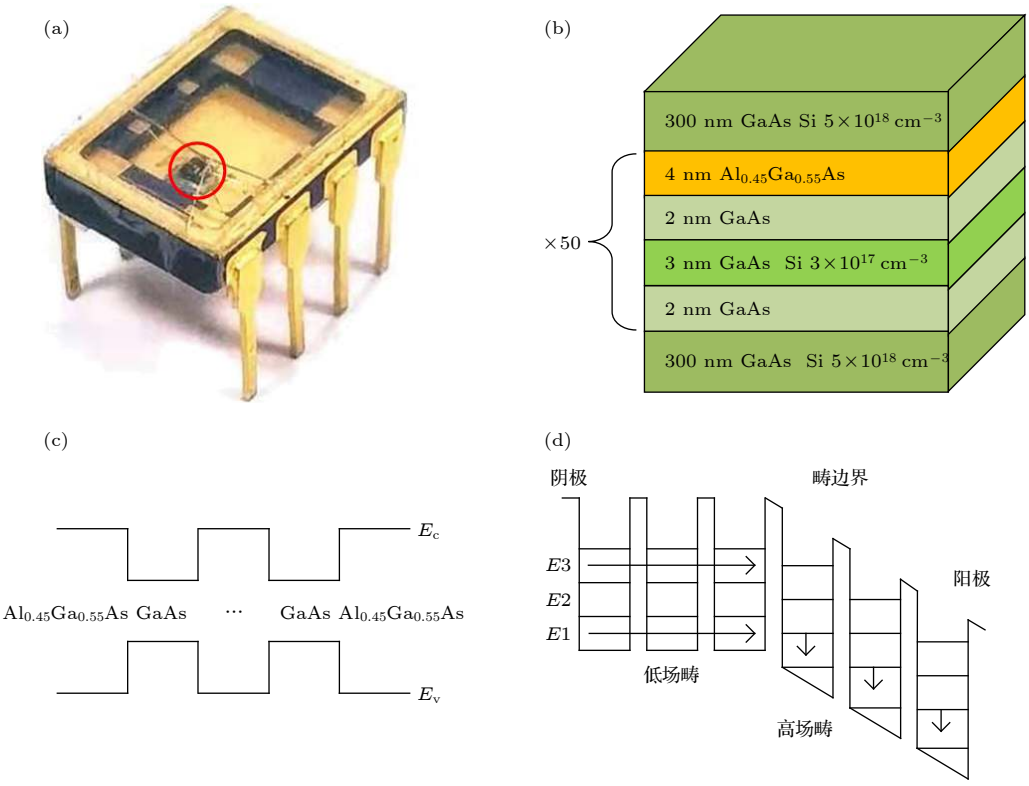

图 1 超晶格 (a) 芯片实物图; (b) 结构示意图; (c) 能带; (d) 高低场畴和级联隧穿模型

Fig. 1. (a) Picture of SLs chip; (b) schematic representation of the SLs device; (c) energy band diagram of SLs; (d) the models of high and low field domain and sequential tunneling of SLs.

振隧穿实现. 图 1(d) 为 SLs 电子运输过程中的级联共振隧穿模型, SLs 加上特定的直流偏置电压, 会使相邻量子阱的子能级间发生级联共振, 即第 n 阱中基态能级与第 n+1 阱中第一激发态子能级相等, 形成共振隧穿. 电荷在外加偏置电压的驱动下, 可以形成电荷的单极子, 即电荷畴. 电荷畴有多种运动方式, 可以朝电场方向或者反方向运动, 产生自发的周期性电流振荡, 这种自发周期振荡被试验验证为是由高低电场畴边界的高频振荡造成的 [24]. 弱耦合 SLs 的级联共振隧穿效应引入了负微分电导效应, 使电场中电子的行为具有非线性特性, 电子失去自身的相位信息, 形成一个非常复杂的随机过程, 因此 SLs 可以被看成是多个互相串联耦合的共振隧穿器件, 即由多个非线性系统互相耦合而成的复杂系统. 共振隧穿效应的强非线性特性引起了 SLs 芯片的自发混沌振荡, 但混沌振荡在理论上仍有待进一步研究 [23].

2.2 SLs 高速物理随机数产生装置

根据 SLs 产生混沌信号的机理, 设计图 2 所示的 SLs 随机数发生器装置. 该系统分为两个部分: SLs 物理熵源部分和随机数提取部分. 物理熵源部分通过选取合适的直流偏置电压产生混沌信号, 随机数提取部分对物理熵源信号采样数字化最终生成随机比特. GaAs/$Al_{0.45}Ga_{0.55}As$ SLs 具有多个能产生自发混沌振荡的直流偏置电压区间, 但是范围较窄, 通常只有几十 mV 左右, 对偏置电压较为敏感 [25], 稍有变化就会使输出混沌信号的基本特性发生变化. 高精度可调直流电源 (high accuracy power supply, HAPS) 可以实时调节输出的电压与电流, 因此本文使用 Keithley 2280S 的 HAPS 进行 SLs 随机数实验. 为避免寄生电容对高频信号带来的影响 [26], 直流偏置需要先经过一个 Bias-Tee 偏置器 (BT), 它由超带宽、接近理想化的电感 L 和电容 C 组成, 其中电感用于隔离交流信号防止高频信号泄露到直流供电系统, 电容用于阻隔直流防止直流电压泄露到高频电路和测量仪器中. 物理熵源部分之间的连线均使用带宽为 6 GHz 的 SMA 高频同轴电缆, SLs 通过 SMA 同轴电缆连接 BT 获得供电, 再经 50 Ω 的 SMA 铜镍同轴负载实现电阻匹配后接地. 从 BT 的电容端引出两路 SLs 信号 C1 和 C2, 第一路信号 C1 供示波器 (OSC, Lecroy, HDO 9404-MS, 40 GS/s) 和矢量网络分析仪 (VNA, Rohde & Schwarz, ZNL6,

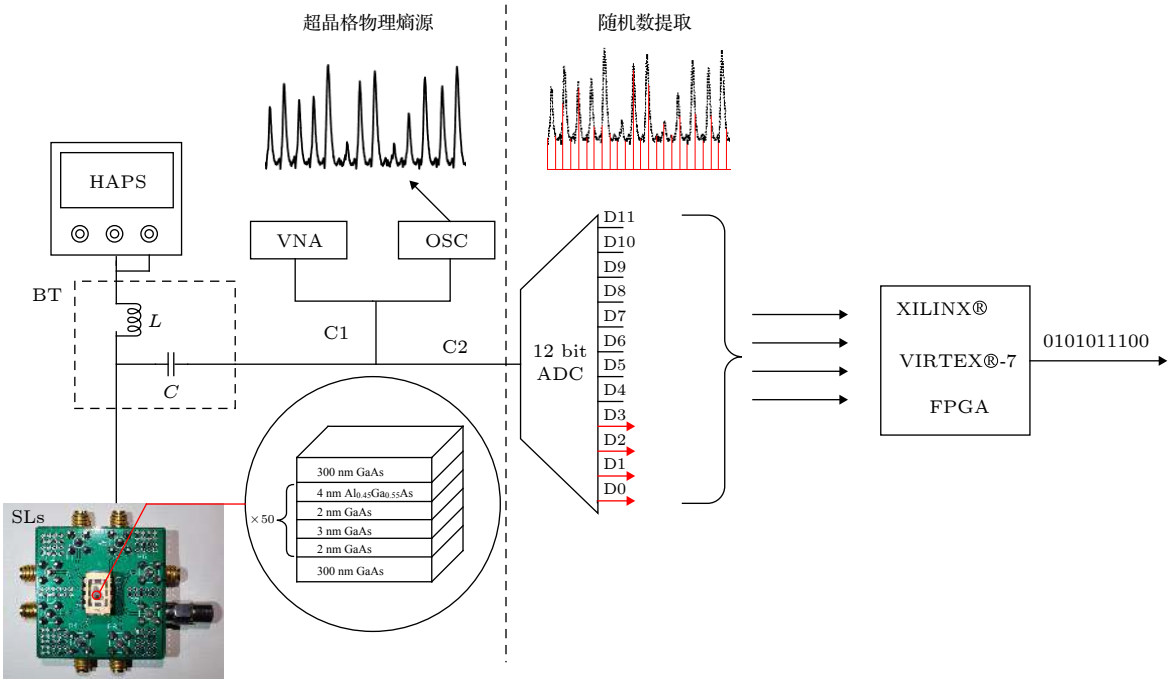

图 2 超晶格高速物理随机数产生装置 (HAPS, 高精度电源; BT, T 型偏置器; SLs, 超晶格; L, 电感; C, 电容; OSC, 示波器; VNA, 矢量网络分析仪; ADC, 模数转化器; FPGA, 现场可编程逻辑门阵列)

Fig. 2. Schematic for high speed physical random number generator of SLs (HAPS, high accuracy powersupply; BT, Bias-Tee; SLs, superlattices; L, inductance (unit Lenz); C, capacitance; OSC, oscilloscope; VNA, vector network analyzer; ADC, analog digital converter; FPGA, field programmable gate array).

5 kHz—6 GHz) 观察和测量 SLs 信号的波形和功率谱, 然后对信号 C2 使用采样频率为 2 GHz 的 12-bit 高速ADC 进行采样量化, 送至FPGA(Virtex-7 XC7VX690T) 进行后处理. FPGA 控制高速 ADC 对 SLs 混沌信号进行采样, 并抽取其中低 4 位作为有效位, 将两个 4 bit 数据合成 8 bit 后进行比特反转, 再将原始序列与经过比特反转的序列再进行异或处理, 最终得到可以输出的随机序列.

3 SLs 自发振荡混沌信号分析

3.1 SLs 信号基本特征

$GaAs/Al_{0.45}Ga_{0.55}As$ SLs 在不同的直流偏置电压下输出的信号具有不同特征, 因此对 SLs 的 *I-V* 特性进行测试, 得到如图 3 所示的 *I-V* 特性曲线图. 根据不同电压区间产生的信号的特征, 将电压区间分为 A, B1, B2 和 C 四个区间.

当实验所用 SLs 处于电压区间 A(0—0.74 V 和 4.40—7.00 V) 时, 几乎无输出信号. 当给 SLs 施加 B1 区间 (0.75—2.27 V) 电压时, 输出单峰周期性信号, 尽管电压幅值随着电压发生变化, 但是其形状在该区间内基本保持一致, 当选取该区间内任一电压值 (如 1.89 V) 时, 可得到该电压下的时序图, 如图 4(a) 所示, 对应电压下的峰峰值在 108 mV 左右. 当 SLs 处于区间 B2(2.28—4.39 V)

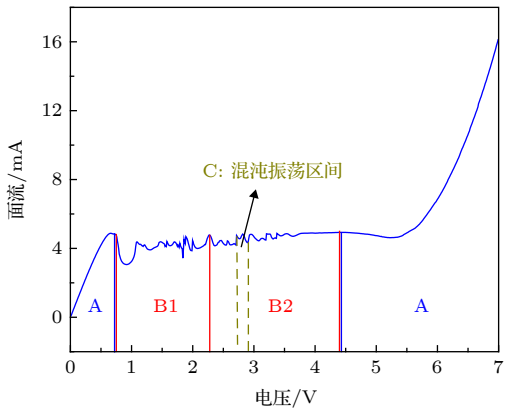

图 3 超晶格 *I-V* 特性曲线

Fig. 3. *I-V* characteristic curve of SLs.

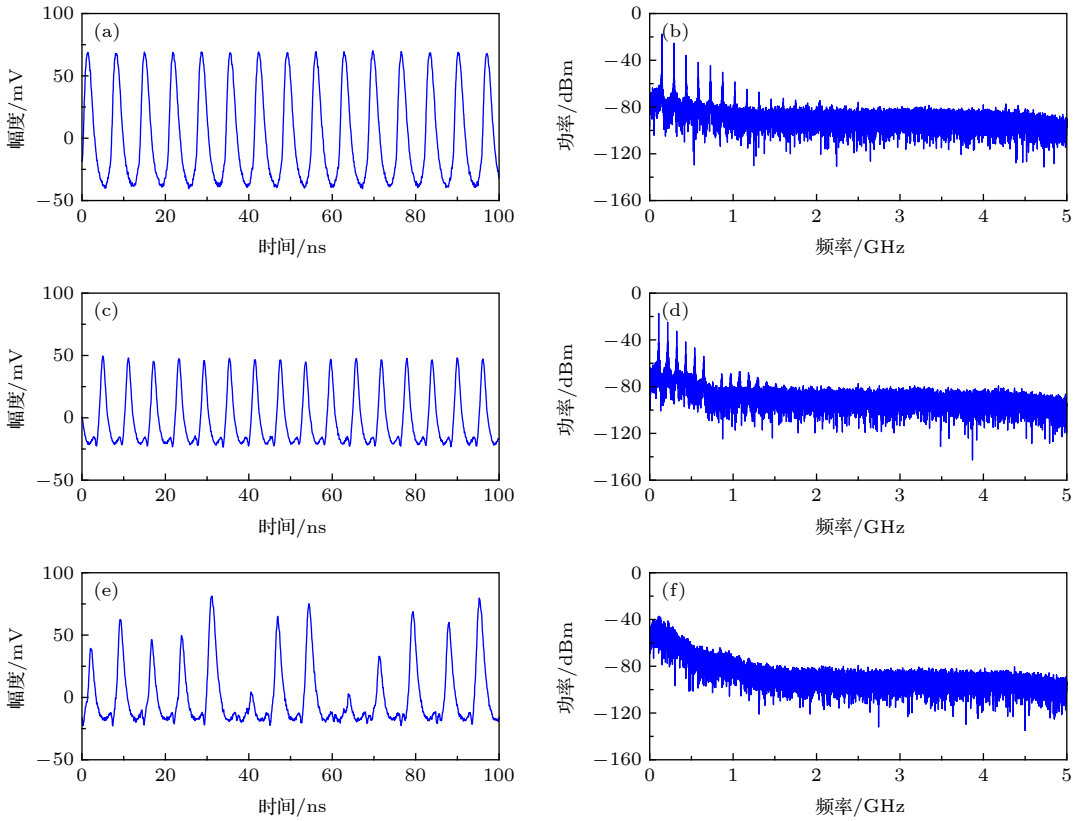

图 4 超晶格 (a) 单峰信号时序图; (b) 双峰信号时序图; (c) 非周期信号时序图; (d) 单峰信号功率谱; (e) 双峰信号功率谱; (f) 非周期信号功率谱

Fig. 4. Superlattices: (a) Temporal waveform of single peak signal; (b) temporal waveform of bimodal signal; (c) temporal waveform of non-periodic signal; (d) power spectrum of single peak signal; (e) power spectrum of single bimodal signal; (f) power spectrum of single non-periodic signal.

时 (除混沌振荡区间), 幅值随电压变化, 但信号形状仍然基本保持一致, 为一大一小双峰周期性信号, 选择该区间的任一电压值 (如 2.42 V) 可得时序图 4(b), 对应的峰峰值在 69 mV 左右. 这两种电压区间下采集的信号不仅在时域上表现出明显的周期性, 在功率谱 (图 4(d) 和图 4(e)) 上也表现出明显非正弦周期性信号的特征, 即高次谐波处出现功率高峰值. SLs 主要的载流子输运是从一个势阱通过势垒隧穿到相邻的势阱, 当加外加偏置电压从低到高逐渐增加时, 特定的电压会使相邻阱间的子能级发生从非共振到共振再到非共振的过程, 从而产生负微分电导效应. 因此除前面提到的几种电压区间, 还存在着一些特殊的负微分电压区间, 电流随电压变大反而变小, 并且在这些电压区间内的 SLs 信号具有非周期信号特征[22,24]. 选择混沌振荡区间 C(2.71—2.90 V) 的负微分区间的某一电压 (如 2.8 V) 时得到时序图 4(c), 其幅度随时间变化并无明显规律出现, 此电压下的 SLs 信号峰峰值在 100 mV 左右, 功率谱 (图 4(f)) 展现的频谱缓而宽, 无高次谐波, 为非周期信号特征[27]. 半导体中的不稳定现象和混沌行为从宏观上来看通常是由于负微分电导特性引起的[28]. 正常情况下半导体中的电流随电压的增大而增大, 而由于 SLs 电子的共振隧穿效应, 导致负微分电导效应, 在负微分电压区间电流随电压增大反而减少, 因此在某些特殊的负微分电导区间 (混沌振荡区间内), 只需给予 SLs 合适直流偏置电压, 便可观察到持续不断的自激振荡混沌信号.

对处于混沌振荡区间的 SLs 信号进行自相关系数计算, 得到其自相关曲线, 如图 5 所示, 经过零时刻峰值处时, 自相关性迅速衰减, 在 2.23 ns 内自相关系数首次衰减至 0.01, 而后逐渐稳定在 0.01 以下, 表明该信号几乎没有自相关性, 说明 SLs 信号没有可检测的周期性[13], 可作为产生随机数的熵源.

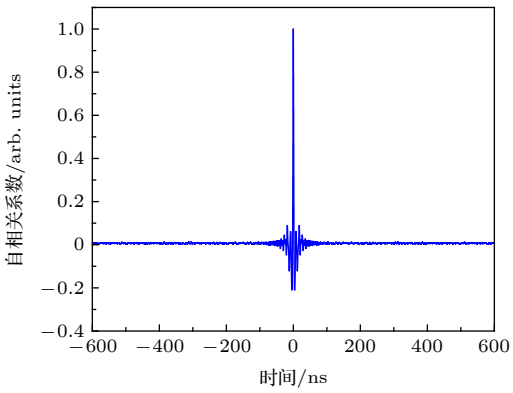

图 5 超晶格信号自相关曲线

Fig. 5. Autocorrelation curve of SLs.

3.2 SLs 信号混沌特性分析

随机数的质量取决于 SLs 产生的混沌信号, 而 SLs 在不同电压下输出的混沌信号特征具有很大不同, 因此, 对不同电压下 SLs 混沌信号的分析显得尤为重要[29,30]. 混沌系统的基本特点就是对运动初始条件的极端敏感性[31], 两个靠得很近的初值所产生的轨线, 随着时间的推移, 将按指数方式分离 (或接近)[32]. 李雅普诺夫指数[33] (Lyapunov exponents, LEs) 是衡量系统动力学特性的一个重要定量指标, 它表征了系统在相空间中相邻轨道间收敛或发散的平均指数率. 利用时间延迟 τ 和嵌入维 m 进行相空间重构而后利用 wolf 法[33] 计算 LEs. 时间延迟 τ 和嵌入维 m 的选择在相空间重构中至关重要, 直接决定了相空间重构后对其以吸引

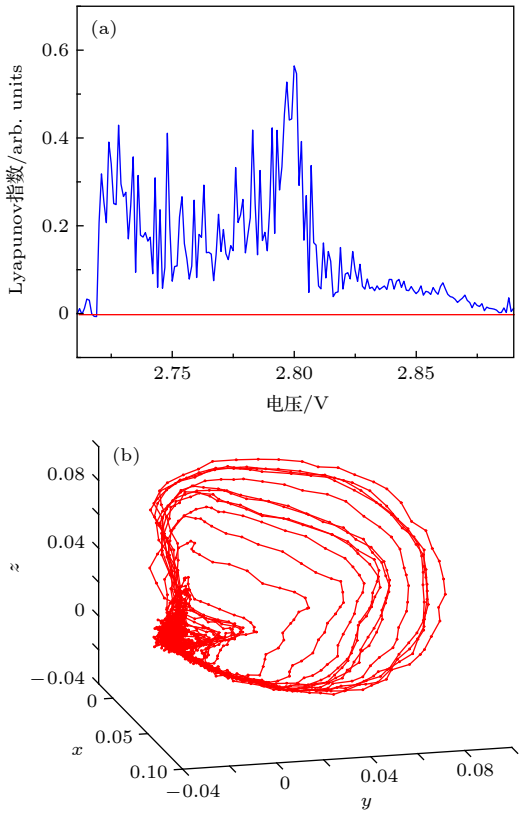

图 6 (a) 不同电压下超晶格信号的最大 Lyapunov 指数; (b) 重构相空间

Fig. 6. (a) The maximum Lyapunov exponents of the superlattices signal at different voltages; (b) the phase space of the superlattices signal.

子的特征描述的不变量的准确度. 本文使用 Masayuki Otani 等提出的自动算法, 该方法利用平均位移法和 Γ-test[34] 联合算法计算时间延迟 τ 和嵌入维 m. 计算混沌振荡区间 (2.71—2.90 V) SLs 混沌信号的最大 LEs, 绘制如图 6(a) 所示的曲线. 对于系统是否存在动力学混沌, 只要最大 LEs 大于零, 就可以确定存在混沌[35]. 为了能够使用混沌程度更高的信号产生随机数, 测试在不同 LEs 的 SLs 信号最终生成随机数的结果, 下文中会给出不同 LEs 的信号生成随机数的测试结果. 图 6(a) 中曲线最高点对应的直流偏置为 2.803 V, 使用该电压下的 SLs 信号进行相空间重构, 并选取其中三个维度绘制如图 6(b) 所示的三维空间曲线图, 从图 6(b) 可以观察到奇异吸引子[36] 的存在. 综上所述, SLs 信号中存在非周期的无规律运动形态, 并且本文所用 SLs 在 2.803 V 电压下具有更强的混沌信号特征.

4 随机数提取与测评

直接将 SLs 信号采样量化输出为随机数, 这样得到的随机数的随机特性并不好. 为了弥补输出分布的不均匀性并进一步消除自相关性, 选择最低最有效位 (least significant bits, LSB) 是一种比较常见的改善分布均匀性的方法[1,37,38]. Kanter 等[13] 和 Nguimdo 等[39] 选择低 4 位作为有效位产生随机数, Hirano 等[40] 选择低 6 位, Li 等[41] 选择低 3 位, 他们通过选取 mLSB, 得到了分布均匀的随机数. 图 7((a)—(d)) 分别展示了当 m 取 8, 6, 5, 4 时, 对应的概率密度分布的变化过程. 与文献 [38,42] 描述一致, 当不断丢弃更多高位, 选择更少的 LSB 位时, 概率密度分布逐渐得到改善. Oliver 等[42] 指出选择合适的比特数可以通过绘制选择不同位数的幅值概率密度分布直方图来估计, 依次降低 m 的值, 直到在允许的统计变化范围内得到一个平坦的直方图. 当选择 $m = 4$ 时, 得到量化结果的幅值分布与均匀分布已基本达到一致. 多位 ADC 量化输出结果有效位数的选取是优质随机数产生的关键[15], 因此在提取 mLSB 作为随机数输出时, 要在满足量化结果幅值分布均衡的前提下尽可能使 m 的值更大, 这样在满足随机性才能同时保证高速率随机数的生成.

值得注意的是, 使用上述方法选择低 4 位所获得的随机比特并不能通过所有的随机性统计检验, 这是因为在生成的随机比特中仍然存在明显的偏差或相关性[38]. 有效位抽取可在一定程度上消除

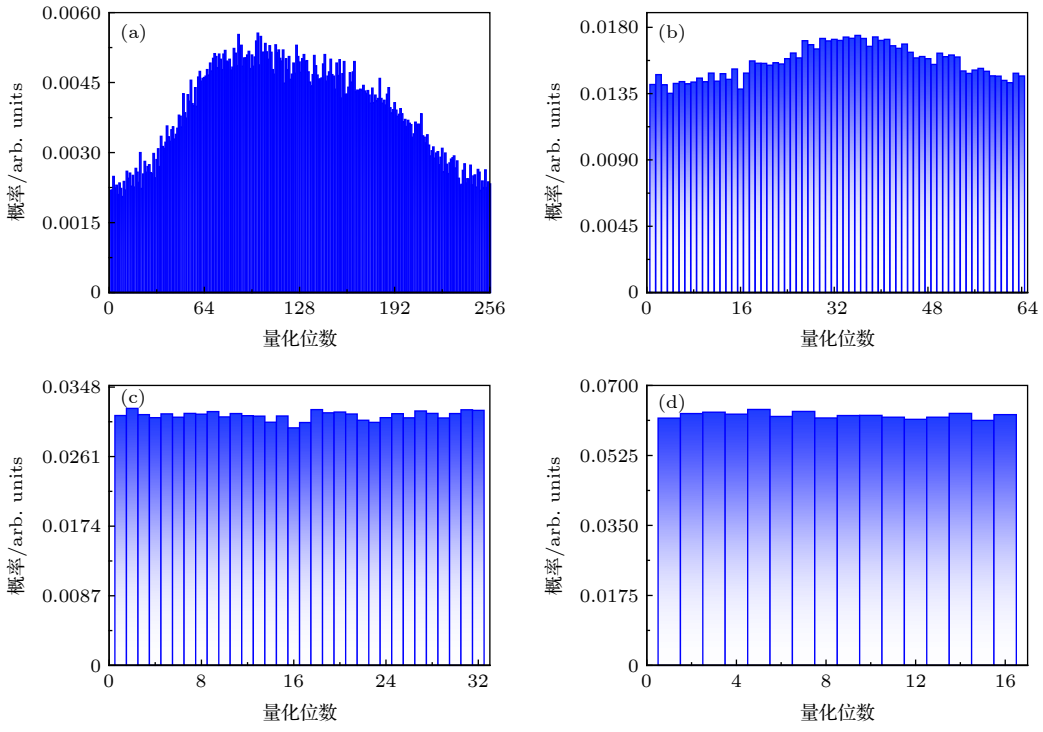

图 7 选取低 m 位有效的概率密度分布 (a) $m = 8$; (b) $m = 6$; (c) $m = 5$; (d) $m = 4$

Fig. 7. M-bit effective probability density distribution: (a) $m = 8$; (b) $m = 6$; (c) $m = 5$; (d) $m = 4$.

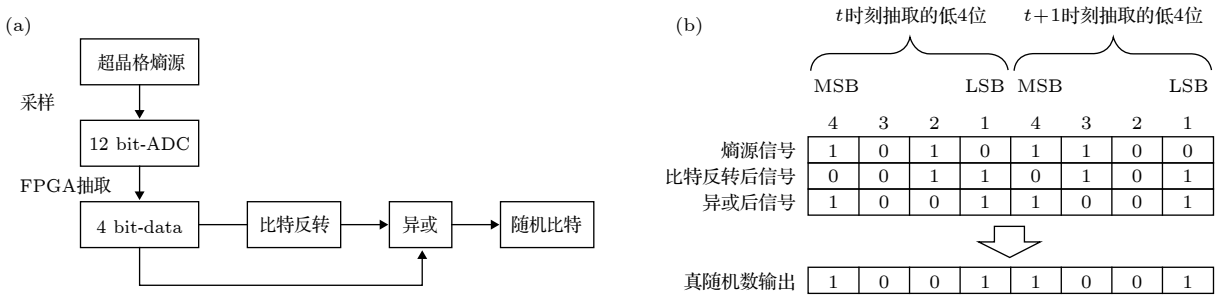

图 8 超晶格量化采集方案 (a) 采集转化原理图; (b) 后处理方案示意图

Fig. 8. acquisition scheme of SLs: (a) Schematic diagram of acquisition conversion; (b) schematic diagram of postprocessing.

偏差和相关性[37,38], Sciamanna 和 Shore[43] 提出除使用 mLSB 方法还需结合其他后处理, 如异或、求导或者比特反转等方法才能最终生成理想随机数. 此前文献 [13, 23, 38] 大多采用离线生成真随机数, 将采集的数据先经过差分后进行一定延迟后与原始数据进行异或, 该方法可以降低随机比特的偏差和相关性, 然后得到优质随机数. 但是使用 12 bit 高速 ADC 得到的超大数据流会导致很难实时完成多阶差分以及延迟等运算处理, 因此无法直接使用离线处理中所使用的方法. 为了进一步提高随机性, 采用比特反转[38] 的方法, 量化采集方案如图 8(a) 所示, SLs 混沌信号采样量化之后得到 12 位的随机比特, 抽取最低 4 bit 作为有效位, 将相邻周期的两个 4 bit 数据拼接为 8 bit 进行比特反转, 最后将原始比特与反转后比特进行异或输出真随机数. 图 8(b) 给出了比特反转和异或的具体操作. FPGA 内部无需对比特反转进行额外运算, 能高速处理 ADC 采集的数据, 实时生成随机数. 使用比特反转的方法可以进一步消除偏差和相关性, 极大地提高了随机比特的生成速度[44], 同时解决了高速数据处理的问题.

采用随机数国际行业测试标准 (NIST SP 800-22) 对生成的随机数进行测试. 该随机数标准测试包含 15 个子项, 每个子项都会有一个 P 值作为其单项测试的结果, 若 P 值大于显著水平 0.01, 则说明该随机数序列通过了相应的测试项, 并且该值越接近 1 说明该项测试中的结果越好. 前文中, 只是计算出了不同电压下 SLs 信号的最大 LEs, 并未经过实际检验说明 LEs 越大的信号可能更适合用于随机数产生. 选取多组不同 LEs 的 SLs 信号, 每个 LEs 的信号分成 1000 组 1 Mbits 的随机数进行测试, 本文给出三组不同 LEs (分别为 0.2, 0.4, 0.56) 信号生成的随机数进行随机数标准测试, 其测试对应的 P 值如图 9 所示, 横坐标轴上的数字 1—15 代表 NIST 测试的 15 个测试项 (具体见表 1). 可以观察到, 不同 LEs 在随机数测试中的 P-value

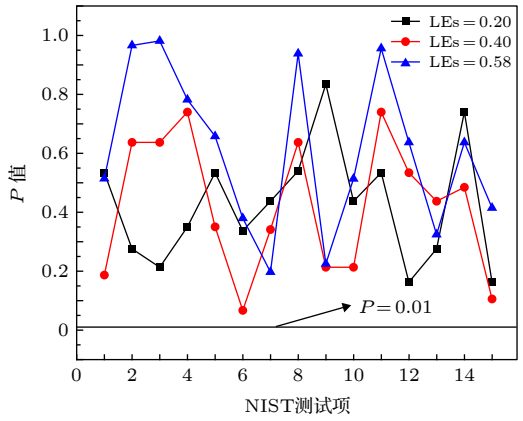

图 9 不同 LEs 的超晶格随机数的 NIST 测试结果

Fig. 9. Results of NIST for superlatticesrandom numbers at different Les.

表 1 NIST 随机特性测试结果

Table 1. Results of NIST statistical test.

统计测试	P 值	通过百分比	结果
频率测试	0.514124	0.995	通过
块内频率测试	0.966244	0.990	通过
累加和测试	0.981609	0.993	通过
游程测试	0.782040	0.993	通过
块内长游程测试	0.657933	0.996	通过
二进制矩阵秩测试	0.379555	0.992	通过
离散傅里叶变换测试	0.196920	0.985	通过
非重叠模块匹配测试	0.938463	0.988	通过
重叠块比配测试	0.224821	0.987	通过
全局通用统计测试	0.513309	0.989	通过
近似熵测试	0.955835	0.998	通过
随机游动测试	0.637119	0.985	通过
随机游动变量测试	0.324180	0.986	通过
串行测试	0.637119	0.982	通过
线性复杂度测试	0.414525	0.995	通过

值具有明显差异, LEs 为 0.2 和 0.4 时的测试结果相差不大, 但仍然可以观察到 LEs = 0.4 时的曲线有更多点位于 LEs = 0.2 的曲线上方, 而 LEs = 0.56 曲线的大多数项测试结果点处于最上方, 从一定程度上反映了 LEs 越大的 SLs 信号, 生成的随机数质量越好. 表 1 为 2.803 V (LEs_{max} = 0.56) 电压下生成的随机数的 NIST 详细测试结果, 包含 P 值和通过测试项的百分比和结果. 从测试结果来看, 本文的随机数发生器产生的随机序列能够通过 15 项随机性测试, 说明通过 SLs 信号产生的随机数具有良好的统计随机性, 其中块内频率测试 (1 Mbit 子块中 0, 1 比例均衡程度) 和近似熵测试 (序列的无规则性) 测试结果几乎达到了 1, 并且整体通过率均大于 0.9806[45], 本文使用 SLs 信号生成的随机数通过了 NIST SP 800-22 的全部 15 项测试.

5 结 论

本文实现了一种基于 SLs 芯片自发混沌振荡现象的实时高速物理真随机数发生器. 该随机数发生器拥有极高的随机数产生速率, 并且具有微型化、易集成、低功耗、系统简单等优点. 使用混沌理论对 SLs 进行分析, 通过 LEs 刻画 SLs 信号的混沌程度, 得到了适合生成随机数的 SLs 电压区间, 并选取相对最佳的直流偏置电压激励 SLs 产生混沌信号, 然后利用采样率为 2 GHz 的 12 位 ADC 对该信号采样量化, 生成多位有效位的随机比特, 通过 FPGA 实时抽取最低 4 位作为有效位, 经过比特反转、异或, 最终实时产生了速率为 8 Gbit/s 的真随机数, 并通过了行业标准 NIST SP 800-22 的测试. 该真随机数发生器兼具高速率与微型化, 有望集成到高速通信设备之上.

感谢中国科学院苏州纳米所张耀辉团队为本文提供的 SLs 器件及理论帮助.

参考文献

[1] 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

[2] Karakaya B, Çelik V, Gülten A 2017 *Int. J. Circuit Theory Appl.* **45** 1885

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

[4] Guo H, Liu Y, Dang A H, Wei W 2009 *Chin. Sci. Bull.* **54** 3651

[5] Arslan T S, Kaya T 2018 *Comput. Math. Methods Med.* **2018** 3579275

[6] Kim J, Nili H, Truong N D, Ahmed T, Yang J, Jeong D S, Sriram S, Ranasinghe D C, Ippolito S, Chun H, Kavehei O 2019 *IEEE Trans. Circuits Syst. I Regul. Pap.* **66** 2615

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

[8] Yamanashi Y, Yoshikawa N 2009 *IEEE Trans. Appl. Supercond.* **19** 630

[9] Wang P j, Li Z, Li G, Cheng X, Zhang H H 2019 *Acta Elec. Sin.* **47** 417 (in Chinese) [汪鹏君, 李桢, 李刚, 程旭, 张会红 2019 电子学报 **47** 417]

[10] Chen J X, Ran L, Chen K 2001 *J. Electron.* **18** 56

[11] Pareschi F, Setti G, Rovatti R 2006 *Proceedings of the 32nd European Solid-State Circuits Conference* Montreaux, Switzerland, September 19–21, 2006 pp130–133

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

[13] Kanter I, Aviad Y, Reidler I, Cohen E, Rosenbluh M 2009 *Nat. Photonics* **4** 58

[14] Wang L S, Zhao T, Wang D M, Wu D Y, Zhou 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]

[15] 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** 30503 (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** 30503]

[16] Esaki L, Chang L L 1974 *Phys. Rev. Lett.* **33** 495

[17] Zhang Y H, Kastrup J, Klann R, Ploog K H, Grahn H T 1996 *Phys. Rev. Lett.* **77** 3001

[18] Wu J Q, Jiang D S, Sun B Q 1999 *Phys. E* **4** 137

[19] Huang Y, Li W, Ma W, Qin H, Zhang Y H 2012 *Chin. Sci. Bull.* **57** 2070

[20] Barkissy D, Nafidi A, Boutramine A, Benchtaber N, Khalal A, El Gouti T 2016 *Appl. Phys. A* 123

[21] Huang Y, Qin H, Li W, Lu S, Dong J, Grahn H T, Zhang Y 2014 *Europhys. Lett.* **105** 47005

[22] Li W, Aviad Y, Reidler I, Song H, Huang Y, Biermann K, Rosenbluh M, Zhang Y, Grahn H T, Kanter I 2015 *Europhys. Lett.* 1123

[23] Li W, Reidler I, Aviad Y, Huang Y, Song H, Zhang Y, Rosenbluh M, Kanter I 2013 *Phys. Rev. Lett.* **111** 044102

[24] Grahn H, Kastrup J, Ploog K, Bonilla L, Galán J, Kindelan M, Moscoso M 1995 *Jpn. J. Appl. Phys.* **34** 4526

[25] Zhang Y, Klann R, Grahn H T, Ploog K H 1997 *Superlattices Microstruct.* **21** 565

[26] Gettings C, Speake C C 2019 *Rev. Sci. Instrum.* **90** 025004

[27] Li Y, Ding Y, Li T 2016 *Chemom. Intell. Lab. Syst.* **156** 157

[28] Tan P A, Zhang B, Qiu D Y 2010 *Acta Phys. Sin.* **59** 3747 (in Chinese) [谭平安, 张波, 丘东元 2010 物理学报 **59** 3747]

[29] Liu Y F, Yang D D, Zheng H, Wang L X 2017 *Chin. Phys. B* **26** 120502

[30] Liu Y F, Yang D D, Wang L X, Li Q 2018 *Chin. Phys. Lett.* **35** 046801

[31] Callan K E, Illing L, Gao Z, Gauthier D J, Scholl E 2010 *Phys. Rev. Lett.* **104** 113901

[32] Lorenz E N 1963 *J. Atmos. Sci.* **20** 130

[33] Wolf A, Swift J B, Swinney H L, Vastano J A 1985 *Physica D* **16** 285

[34] Stefánsson A, Končar N, Jones A J 1997 *Neural Comput.*

Appl. **5** 131
[35] Vicente R, Dauden J, Colet P, Toral R 2005 *IEEE J. Quantum Electron.* **41** 541
[36] Takens F 1981 *Dynamical Systems and Turbulence* (Heidelberg: Springer Press) pp366–381
[37] Hirano K, Amano K, Uchida A, Naito S, Inoue M, Yoshimori S, Yoshimura K, Davis P 2009 *IEEE J. Quantum Electron.* **45** 1367
[38] Li N, Kim B, Chizhevsky V N, Locquet A, Bloch M, Citrin D S, Pan W 2014 *Opt. Express* **22** 6634
[39] Nguimdo R M, Verschaffelt G, Danckaert J, Leijtens X, Bolk J, van der Sande G 2012 *Opt. Express* **20** 28603
[40] 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
[41] Li X Z, Chan S C 2012 *Opt. Lett* **37** 2163
[42] Oliver N, Soriano M C, Sukow D W, Fischer I 2013 *IEEE J. Quantum Electron.* **49** 910
[43] Sciamanna M, Shore K A 2015 *Nat. Photonics* **9** 151
[44] Akizawa Y, Yamazaki T, Uchida A, Harayama T, Sunada S, Arai K, Yoshimura K, Davis P 2012 *IEEE Photonics Technol. Lett.* **24** 1042
[45] 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]

Generation of 8 Gb/s physical random numbers based on spontaneous chaotic oscillation of $GaAs/Al_{0.45}Ga_{0.55}As$ superlattices*

Liu Yan-Fei [1)] Chen Cheng [1)] Yang Dong-Dong [1)†] Li Xiu-Jian [2)]

1) (*Department of Basic Courses, Rocket Forces Engineering University, Xi'an* 710025, *China*)

2) (*College of Liberal Arts and Sciences, National University of Defense Technology, Changsha* 410073, *China*)

(Received 19 January 2020; revised manuscript received 14 March 2020)

Abstract

Secret key is required in secure communications, and random numbers are generally used as keys to encrypt the original information. So it is crucial for cryptography and secure communication to generate the physical random number, which is completely safer than pseudo random number. However, Existing physical random number generator systems are difficult to satisfy the requirements of high-speed communication due to their complexity, large size, and limited equipment bandwidth. The $GaAs/Al_{0.45}Ga_{0.55}$ superlattices is based on a structure formed by the alternating growth of two semiconductor materials, and has a good low-dimensional structure for studying the nonlinear behavior of electrons. Recent studies have shown that the $GaAs/Al_{0.45}Ga_{0.55}$ superlattices under the DC voltage could appear chaos current oscillation states in some certain voltage ranges.

An all-solid-state real-time high-speed physical true random number generator based on superlattices is presented. The superlattices, excited by appropriate DC bias voltage, could generate a high-frequency chaotic oscillation signal as a source of physical entropy. A multi-bit analog-to-digital converter with 2 GHz sampling frequency is used for quantization to generate 12-bit binary random bits. Then, the field programmable gate array extracts the lowest 4 bits as valid bits and inverts bits to improve its randomness, and finally a true random number with a real-time rate of 8 Gbit/s is obtained. To obtained a superlattices signal with a higher degree of chaos, the Lyapunov exponent was used to assist in selecting a more suitable DC bias. The random number generated by the superlattices, owning excellent statistical characteristics, could pass the test of the random number industry standard (NIST SP 800-22), which is expected to be miniaturized and integrated on high-speed communication equipment.

Keywords: superlattices, spontaneous chaotic oscillation, physical true random numbers, multibitsample

PACS: 05.40.–a, 73.21.Cd, 05.45.–a, 68.65.Cd **DOI:** 10.7498/aps.69.20200136

* Project supported by the Key Program of the National Natural Science Foundation of China (Grant No. 61834004).

† Corresponding author. E-mail: yd_xian@163.com