DOI:10.19651/j.cnki.emt.2106294

基于 GaAs/AlGaAs 超晶格受激混沌振荡的随机数发生器设计与实现*

应杰攀[1,2] 宋贺伦[1] 罗晓朋[3]
(1.中国科学院 苏州纳米技术与纳米仿生研究所 苏州 215123;2.中国科学技术大学 纳米科学技术学院 苏州 215000;
3.火箭军工程大学基础部 西安 710025)

摘 要:针对伪随机数在密码应用中存在的安全性问题,基于超晶格物理熵源的特性,分析受激混沌作为熵源的优势,首次提出了将超晶格受激混沌振荡作为真随机数发生器熵源,利用 12 位 ADC 实现超晶格受激混沌信号的数字化采样,FPGA 作为后处理单元,设计并实现了一种真随机、高性能、高速度的超晶格随机数发生器,实时生成随机数的速率达 300 Mbit/s,该超晶格随机数性能可通过美国国家标准局所提供的标准(NIST SP 800-22)要求测试,结果表明该超晶格随机数具有良好的随机性。

关键词:超晶格;随机数发生器;物理熵源;后处理;FPGA
中图分类号:TN911.2 **文献标识码**:A **国家标准学科分类代码**:510.3030

Design and implementation of random number generator based on stimulated chaotic oscillation of GaAs/AlGaAs superlattice

Ying Jiepan[1,2] Song Helun[1] Luo Xiaopeng[3]
(1. Suzhou Institute of Nano-Tech and Nano-Bionics, Chinese Academy of Science, Suzhou 215123, China;
2. Nano Science and Technology Institute, University of Science and Technology of China, Suzhou 215000, China;
3. Basis Department, Rocket Force University of Engineering, Xi'an 710025, China)

Abstract: Aiming at the security problem of pseudo-random number in cryptographic applications, based on the characteristics of superlattice physical entropy source, this paper analyzes the advantages of stimulated chaos as entropy source, and proposes for the first time that the stimulated chaos oscillation of superlattice is used as entropy source of true random number generator, 12 bit ADC is used to realize digital sampling of stimulated chaos signal of superlattice, and FPGA is used as post-processing unit, a true random, high-performance and high-speed superlattice random number generator is designed and implemented. The real-time generation rate of random number is up to 300 Mbit/s. The performance of the superlattice random number generator can pass the standard (NIST SP 800-22) provided by the National Bureau of standards. The results show that the superlattice random number has good randomness.

Keywords: superlattice; random number generator; physical entropy source; post-processing; FPGA

0 引 言

随着通信技术、计算机网络等新兴技术的迅速发展,信息安全对于人们的生产生活越来越重要[1]。在量子计算[2]和人工智能技术快速发展的时代,传统纯数字意义上的密码算法正在面临着重大的冲击,凭借着智能化、高算力的破解手段,在短时间内破解复杂的数学加密算法已经变得可能。信息安全是信息时代健康、稳定发展的前提,而随机数发生器是信息安全性的根本来源[3],性能优良的随机数发生器技术一直是密码学界的重点攻关方向。

目前市场上,实用型真随机数发生器的物理熵源主要包括热噪声直接放大[4]、振荡器采样[5]、混沌电路[6]等。20 世纪末,Comsciro 公司首次设计并实现了基于热噪声的真随机数发生器,但其生成速率仅有 2 kbit/s。2004 年,浙江

收稿日期:2021-04-04
* 基金项目:中国科学院科技服务网络计划(KFJ-STS-QYZX-061)、纳米真空互联试验站(2018-000052-73-01-000356)、"十三五"国家密码发展基金(MMJJ20180112)项目资助

大学用模拟电路实现了基于混沌电路的真随机数发生器，生成速率达 20 Mbit/s，并通过了 NIST 的检测，成为了实用化真随机数发生器的代表。2011 年，中国科学技术大学设计了一款基于电路抖动的真随机数发生器，利用线性反馈移位寄存器的方法进行后处理，生成速率达到 20 Mbit/s，并适配了 USB 数据传输接口[7]。目前市场上的真随机数发生器技术的物理熵源一直得不到突破，生成速率也大都在 Mbit/s 量级，难以满足当今的高速保密通讯的需求。此外，基于混沌激光和量子效应的真随机数发生器，虽然在带宽和输出速率上都有了显著的提升，但是这些激光和量子系统的复杂性相当高，研发成本较大，而且稳定性尚未达到正常使用水平。目前，可实用、高性能、低成本的真随机数发生器成为了一个较大的空缺。

半导体超晶格是一个接近理想的多自由度的非线性复杂系统[8]，近年来，通过全新的超晶格材料结构设计及工艺方法优化，在国际上率先观测到了半导体超晶格在室温下的高频混沌振荡[9]，其混沌振荡噪声可达百兆及以上，兼备体积小、功耗低(mW 量级)、低成本等优点，其混沌振荡的种种特性符合随机数熵源的一系列要求。2020 年，火箭军工程大学率先将超晶格的自发混沌振荡应用到真随机数发生器的研发中[10]，并取得了巨大的突破。但是在后续的研究中发现，超晶格的自发混沌振荡的电压区间非常窄，并且受温度影响较大，要实现实用化，随机性实时监测和电压自调节模块将变得非常必要，这无疑在增加了系统复杂度的同时，降低了稳定性。

为此，本文在对超晶格熵源特性的研究中，发现超晶格的受激混沌振荡相较于自发混沌振荡具有更高的稳定特性，并首次提出了将受激混沌振荡作为真随机数发生器的熵源，利用 12 位的高速模数转换器(analog-to-digital converter，ADC)进行数字化采样，用现场可编程门阵列(field programmable gate array，FPGA)进行数据后处理，对超晶格原始输出进行 LFSR 的 Toeplitz 随机性提取，完成 300 Mbit/s 的实时速率输出真随机数。最后通过随机性监测，证明超晶格随机数具有较好的性能指标。

1　超晶格物理熵源特性

中等掺杂的弱耦合超晶格是一个多维度的非线性动力学系统，该特征造就了超晶格混沌特性。本文使用的 GaAs/AlGaAs 超晶格由 GaAs 和 AlGaAs 两种不同的材料周期性交替排列而成，如图 1 所示，由于其结构的特殊性，会形成独特的量子阱结构[11]。在合适的外加电压下，会导致量子阱之间的共振隧穿效应，表现出负微分电导，给系统带来巨大的非线性[12]，表现为电流的混沌振荡。本章从超晶格的 I-V 特性、受激输出特性、熵估计角度介绍超晶格受激混沌作为随机数熵源的可行性和优越性。

1.1　I-V 特性分析

在直流偏执下，超晶格表现出多重稳定性，展现为多种

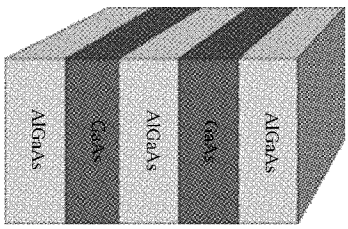

图 1　GaAs/AlGaAs 超晶格材料结构

振荡模式，有自发混沌振荡、无振荡、准周期振荡。在自发混沌振荡和准周期振荡间通过无振荡形式过渡，此时的场畴为准平衡，在外部激励信号作用下，可将该准平衡状态破坏，转变为混沌振荡，故又称之为受激混沌，理论上自发混沌和受激混沌都可以作为随机数熵源。但如图 2 所示的 I-V 特性图，区域 a 为自发混沌区间，区域 b 为受激混沌区间，a 区间非常小，而 b 区域的区间接近 1 V，初步表明了受激混沌的工作点比自发混沌更加容易确定。

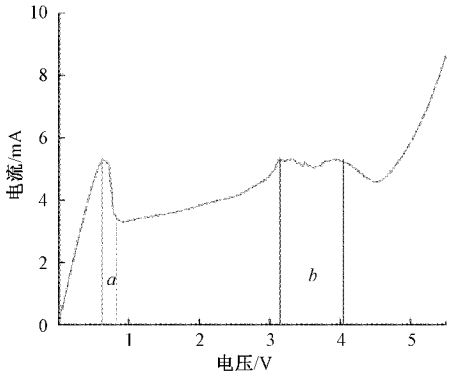

图 2　室温下的超晶格 I-V 特性

在实验中，本文发现超晶格的 I-V 曲线会随着温度发生偏移，如图 3 所示。可以看出，由于自发混沌区间过于小，在温度改变的时候，各个温度之间的自发混沌区间变得没有交集，表明想要维持自发混沌，必须改变偏置电压。而由于受激混沌的区间较大，不管温度如何变化，彼此之间都存在交集，只要合理设置偏置电压，就可以在各个温度下都维持受激混沌振荡。

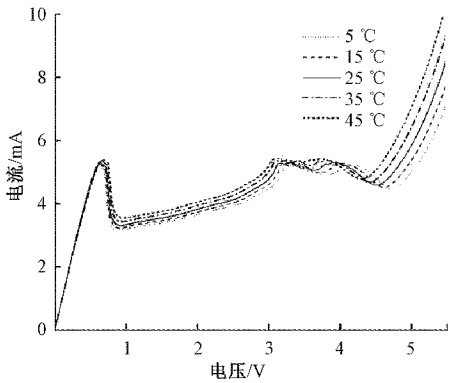

图 3　不同温度下的超晶格 I-V 特性

1.2　受激混沌输出特性

对于混沌和准周期中间的无振荡过渡期间,超晶格的场畴处于准平衡状态,只要稍加改变外部条件就可使其进入混沌状态。本文依照该特性,设计了如图 4 所示的电路图,高频电感用于阻隔超晶格产生的高频信号,避免对高精度稳压电源的影响,高频电容用于阻隔直流信号传输到示波器,影响观测。

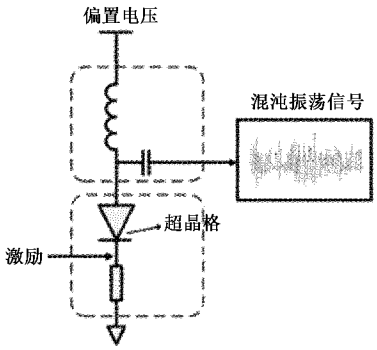

图 4　超晶格受激混沌电路

图 5(a)、(b)分别为超晶格室温下受激混沌振荡的 250 和 25 ns 间隔内的时域谱图,从图 5(a)中可以看出,时域信号总体上较为混乱,并没有规律可循,表明该状态下的振荡没有周期性,具有较好的混沌振荡特性。从图 5(b)中可以看出,时域谱变化间隔在纳秒量级,表明该混沌振荡的变化速率非常快,也就说明能够利用该振荡源实现高速的随机数发生器。

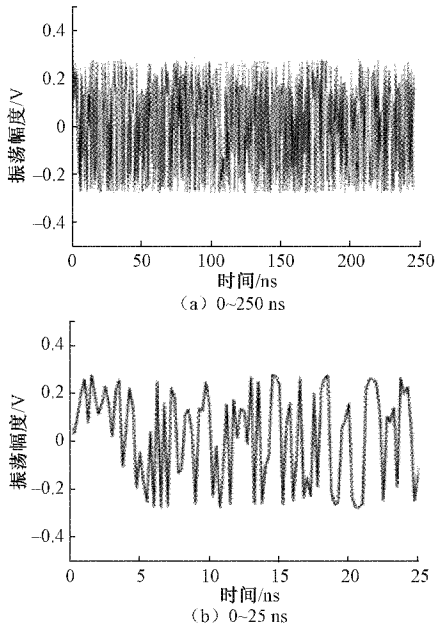

图 5　超晶格器件在室温下的时域振荡特性

图 6 为超晶格器件室温下受激振荡的频域谱图,由频谱图可知,该样本的超晶格的 3 dB 带宽达到了 300 MHz,并且没有观测到周期性的成分,并且振荡处于混乱状态,如此高的带宽突破了大部分物理噪声源的带宽瓶颈,可以当作优质的真随机数熵源来使用。

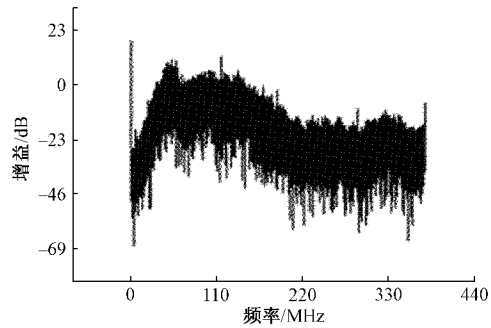

图 6　超晶格器件在室温下受激混沌振荡的频域谱

1.3　熵估计

熵估计是评估熵源混乱度的主要手段,熵值越大,表明数据越混乱,能够提取出的真随机数越多,通过熵估计还可以为后续的后处理提供参数参考。本文采用国际通用的 NIST 800-90B 随机数熵评估套件[13],取该套件中所有评估手段的最小熵值结果作为超晶格熵源的极小熵,每 8 bit 的估熵结果如表 1 所示。极小熵为 7.288,表明每 8 bit 至少可以提取出 7.2 bit 的真随机数,极小熵值较为优越。本文根据此结果,同时保留一定冗余,可以将随机性提取参数设置为 $m/n=6/8$。

表 1　极小熵估计

熵估计方法	极小熵
Most Common Value Estimate	7.984
Collision Estimate	7.288
Markov Estimate	7.963
Compression Estimate	7.424
t-Tuple Estimate	7.394
LRS Estimate	7.973
MultiMCW Prediction Estimate	7.651
Lag Prediction Estimate	7.974
MultiMMC Prediction Estimate	7.288
LZ78Y Prediction Estimate	7.288

2　真随机数发生器系统设计

2.1　采集手段

欠采样是采样型随机数发生器里一种常用的工程实现方案,一方面通过降低采样率可以获得更好的原始随机序列的质量,从而降低后续数字后处理的计算消耗与处理吞吐率需求;另一方面采样率较低的 ADC 为嵌入式系统带来更好的实现便捷性和性价比。针对特定随机数输出速率需要及输出接口性能,来选择合适的 ADC 型号。本文设计方

案中，采用的 ADC 选型为亚德诺（ADI）半导体的 AD9226ARSZ，该 ADC 在 65 MSPS 的采样速率下，可以维持 12 位精度，全带宽输出速率可以达到 750 MHz。在 65 MSPS 的采样速率下，将采样得到的数字序列送到 FPGA 中进行后处理。

2.2　基于 FPGA 的后处理

理想情况下，超晶格混沌振荡的输出具有较好的随机性，但是同其他物理随机数发生器（如量子、激光混沌）一样，受到经典噪声、器件相关性、电压抖动等不良因素影响，超晶格熵源也有相似的缺点：1）原始输出无法达到满熵；2）原始输出的统计特性需要进行改善。需要对超晶格熵源直接采样得到的数字序列进行特定的后处理，才能获得符合特征的真随机数。

FPGA 是纯硬件电路[14]，较为安全，并且功耗低，运算速度快，可以重编译，使用灵活，用 FPGA 进行随机数板子的开发，能有效节约开发成本、时间和功耗。出于综合性考虑，本文选用 Altera Cyclone-Ⅳ E 系列的 FPGA 作为后处理单元。

Krawczyk 提出属于 Universal2 函数族基于 LFSR 的 Toeplitz 矩阵可以用于认证和保密增强工作[15]，并且有数学理论证明其安全性。基于 LFSR 的 Toeplitz 矩阵在 FPGA 中很容易实现，Toeplitz 矩阵相乘的算法也可以充分发挥 FPGA 并行计算的优势。本文采用 LFSR 的 Toeplitz 矩阵对 ADC 采样得到的超晶格初始熵源进行消偏处理，既可以实现无条件安全，也可以获得较大的吞吐量。

本文先对 12 位的 ADC 采样得到的数据进行 8-LSB 数据预处理，LSB 处理能够改善分布的均匀性。然后将该 8 位数据输入与 Toeplitz 矩阵进行相乘，提取器参数按照上文熵估计的结果取 $m/n=6/8$，m 代表了矩阵的列数，n 代表了行数，矩阵中的元素由 LFSR 实时更新，最终将数据进行输出原理如图 7 所示。

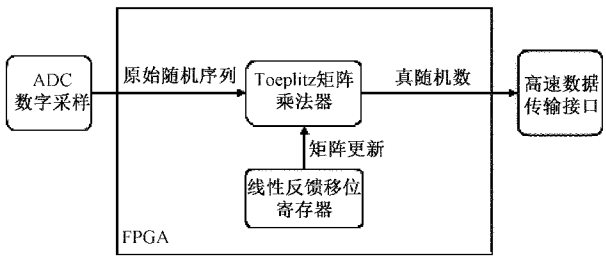

图 7　基于 LFSR 的 Toeplitz 原理

3　随机性检测

对随机数进行检测评估，是检验其随机数发生器是否安全可靠的关键[16]，随机性检测的基本原理就是对随机数发生器生成的随机数进行概率统计，通过概率统计的结果来分析所产生的随机数是否符合随机性检测标准。

本文使用国际通用的 NIST SP 800-22 检测套件对超晶格随机数进行随机性测试，将样本长度设定为 1 000 000 bit，检测的样本数量设置为 1 000。测试结果如表 2 所示。

表 2　1 000 组×1 000 000 的 NIST 检测结果

Statistical Test	P-value	Result
Frequency	0.775 3	通过
Block Frequency	0.141 2	通过
CumulativeSums	0.506 1	通过
Runs	0.741 9	通过
LongestRunofOnes	0.528 1	通过
Rank	0.016 8	通过
FFT	0.901 9	通过
NonOverlapping Template	0.668 3	通过
OverlappingTemplate	0.096 0	通过
Universal	0.805 5	通过
ApproximateEntropy	0.268 9	通过
RandomExcursions(1)	0.098 5	通过
RandomExcursions(−1)	0.106 6	通过
LinearComplexity	0.500 2	通过
Serial(m=16)	0.021 7	通过

NIST SP 800-22 检测套件对 15 个指标进行了检测，P-value 大于显著水平 0.01，表明该指标达标，大于 0.5 则说明该指标非常好。从检测可以看到，15 项检测结果均达标，并且 Frequency、CumulativeSums、Runs 等多数指标达到了较高的水准，直接验证了超晶格随机数发生器的性能。

4　结　　论

本文以超晶格受激混沌振荡为熵源，设计并实现了一种真随机、高性能、高速度的超晶格随机数发生器。通过对超晶格受激混沌振荡的 I-V 曲线、输出响应、极小熵值进行分析，介绍了其作为随机数熵源的优越性，利用 12 位的 ADC 进行数字化采样，以 FPGA 作为后处理单元，实现了基于 LFSR 的 Toeplitz 随机性提取，最终实现了实时输出速率达到 300 Mbit/s 的真随机数输出。并且通过 NIST 检测验证其安全性。超晶格随机数发生器性能突出、成本低廉、稳定性强，在信息安全领域有着十分广阔的应用前景。

参考文献

[1]　薛娟，刘萍. 基于混沌 Gyrator 变换与离散小波变换的多图像光学同步加密算法[J]. 电子测量与仪器学报，2019，33(11)：136-146.

[2]　田国华，胡云瀚，陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报，2021，32(5)：1495-1525.

[3]　唐世彪，程节，栗帅. 高速 QKD 系统的随机数源及实时自检方案研究[J]. 量子电子学报，2021，38(1)：86-93.

[4] 魏子魁,胡毅,金鑫,等.一种低功耗高噪声源真随机数设计[J].电子与信息学报,2020,42(10):2566-2572.

[5] 卜朝晖,常仙云,陈文星,等.基于可触发环形振荡器的高精度时间间隔测量[J].仪器仪表学报,2019,40(5):10-18.

[6] 杨会.数字真随机数发生器的设计与分析[D].西安:西安电子科技大学,2018.

[7] 张鸿飞,王坚,罗春丽,等.基于抖动的高速真随机数发生器的设计和实 现[J].核技术,2011,34(7):556-560.

[8] 张龙,陈张海.激子极化激元光子学研究进展[J].中国科学:物理学 力学 天文学,2021,51(3):17-29.

[9] HUANG Y Y, WEN L, MA W Q. Experimental observation of spontaneous chaotic current oscillations in GaAs/Al0.45Ga0.55As superlattices at room temperature [J]. Chinese Science Bulletin, 2012, 57(17): 2070-2072.

[10] 刘延飞,陈诚,杨东东,等.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[J].物理学报,2020,69(10):140-148.

[11] 洪云.一维等间距 δ 势垒中的波函数及其物理性质[J].重庆工商大学学报(自然科学版),2016,33(5):29-35.

[12] 车相辉,梁士雄,张立森,等.基于 MOCVD 生长材料的高电流密度太赫兹共振隧穿二极管[J].电子技术应用,2019,45(8):32-33,39.

[13] 吴明川,成琛,张江江,等.高速量子随机数产生中的实时并行后处理[J].光通信研究,2020(5):1-6.

[14] 胡荣维,冯龙飞,刘君华,等.一种基于数据压缩传输的高速大满贯测井系统[J].电子测量技术,2021,44(2):71-76.

[15] 袁莉芬,熊波.基于超素数的托普利兹观测矩阵构造方法[J].仪器仪表学报,2015,36(7):1598-1604.

[16] 王彤,朱敏玲.序列检测和近似熵检测的快速实现研究[J].计算机工程与应用,2020,56(15):113-117.

作者简介

应杰攀,硕士研究生,主要研究方向为半导体器件集成化应用。

E-mail:jpy2018@mail.ustc.edu.cn

宋贺伦(通信作者),博士,研究员,主要研究方向为半导体器件集成技术及应用。

E-mail:hlsong2008@sinano.ac.cn

罗晓朋,硕士研究生,主要研究方向为网络空间安全、嵌入式系统设计。

E-mail:Lxppage@163.com